

Advanced approaches
in CyberSecurity
Vatclav Dovnar
HL
HighLoad++
2022

whoami


```
{
  speaker_name: “Vatclav Dovnar”
  skills: [appSec, infraSec, devSecOps,
problem_solving],
  skill_years: 9,
  job_title: “Head of Product Security”,
  tolk_time: 40,
  hiring_status: “Looking for cool teammates”

}
```



profile_photo.png



telegram.png



Thanks to



Иван Васильев



Жания Рахметова



Введение

Организации проектируют системы, которые копируют структуру коммуникаций в этой организации

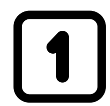


Мелвин Конвей



Введение

Важные выводы:



Команды закрепляют свои
зоны ответственности
на уровне API-интерфейсов



Введение

Важные выводы:

1

Команды закрепляют свои зоны ответственности на уровне API-интерфейсов

2

Решение задач требует кросскомандной коммуникации и ресурсов на нее



Введение

Кто отвечает за безопасность продукта?



Введение

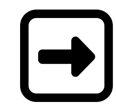
Кто отвечает за безопасность продукта?

ИБ



Введение

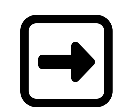
Кто отвечает за безопасность продукта?

ИБ  не является владельцем актива



Введение

Кто отвечает за безопасность продукта?

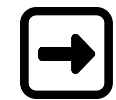
ИБ  не является владельцем актива

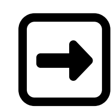
Команда продукта



Введение

Кто отвечает за безопасность продукта?

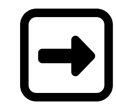
ИБ  не является владельцем актива

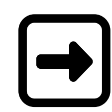
Команда продукта  не разбирается в ИБ



Введение

Кто отвечает за безопасность продукта?

ИБ  не является владельцем актива

Команда продукта  не разбирается в ИБ

Руководство



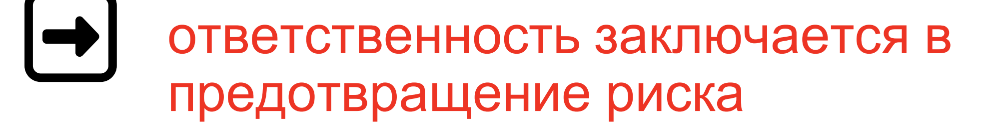
Введение

Кто отвечает за безопасность продукта?

ИБ → не является владельцем актива

Команда продукта → не разбирается в ИБ

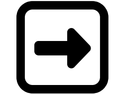
Руководство

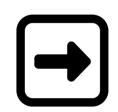


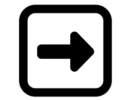


Введение

Кто отвечает за безопасность продукта?

ИБ  платформа, консалтинг, метрики, экспертиза

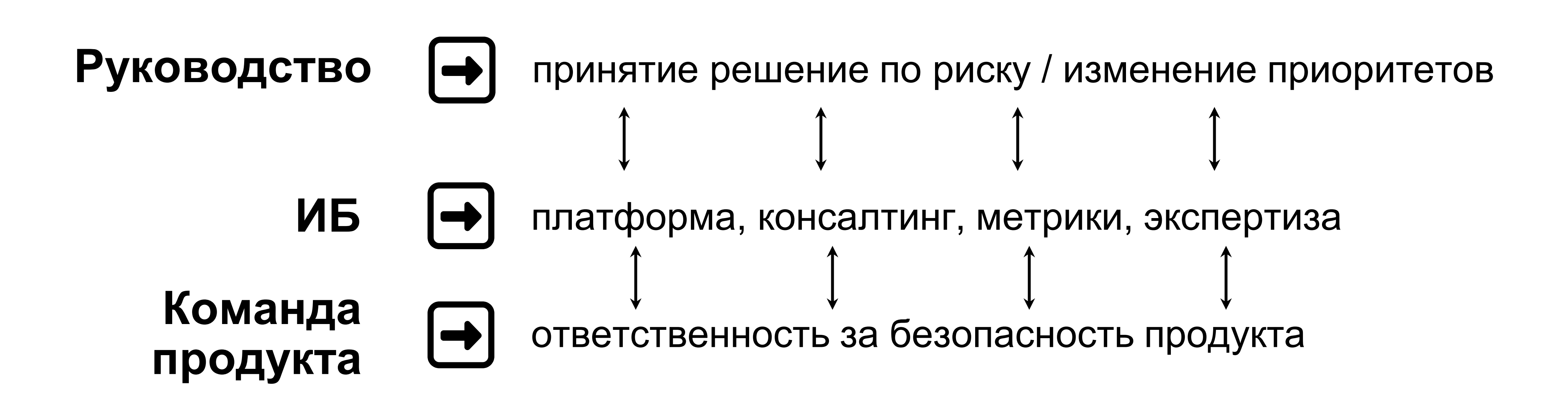
Команда продукта  ответственность за безопасность продукта

Руководство  на основе понятных данных принимает решение о принятии рисков. Контролирует общую картину



Введение

Кто отвечает за безопасность продукта?

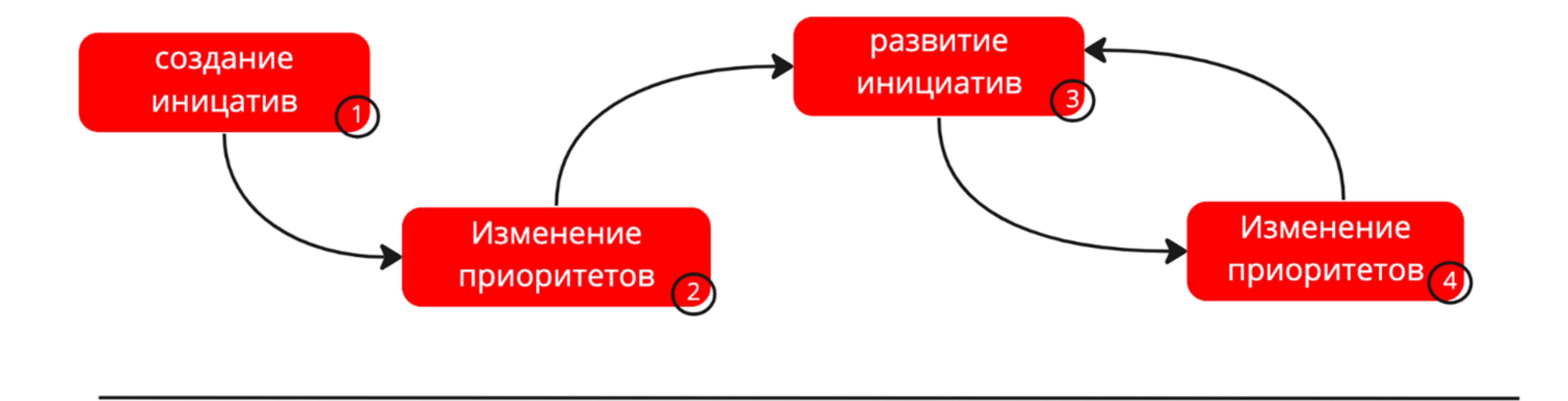




Cyber Strategy



Cyber Strategy





Cyber Strategy

создание инициатив 1

Изменение приоритетов 2

развитие инициатив 3

Изменение приоритетов 4

1 год



Cyber Strategy

создание инцатив 1

Изменение приоритетов 2

развитие инициатив 3

Изменение приоритетов 4

1 месяц

1 месяц



Cyber Strategy

Как ИБ помогает бизнесу?

- Консалтинг по наведению порядка (сети, DNS, список активов, expired TLS)
- Мотивация к избавлению от legacy (старые сети, сервера, версии API, код)
- Увеличение стабильности
- Экосистема инструментов безопасности в пайплайне сборки
- Помощь в росте сотрудников



Cyber Strategy

Как ИБ помогает бизнесу?

- Консалтинг по наведению порядка (сети, DNS, список активов, expired TLS)
- Мотивация к избавлению от legacy (старые сети, сервера, версии API, код)
- Увеличение стабильности
- Экосистема инструментов безопасности в пайплайне сборки
- Помощь в росте сотрудников
- Ваш пункт

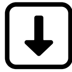


Cyber Strategy

Как ИБ помогает бизнесу?

Помощь

Улучшение коммуникации



Долгосрочное улучшение безопасности





Security error budget



Security error budget

Флоу исправления уязвимостей

ИБ
Поиск и воспроизведение → фиксация в JIRA
фиксация в JIRA → автоматизации
консультации
верификация → написание регресса

Dev
фиксация в JIRA → исправление
консультации → исправление
исправление → верификация



Security error budget

Флоу исправления уязвимостей

автоматизации

ИБ

Поиск и воспроизведение

фиксация в JIRA

консультации

верификация

написание регресса

Dev

исправление



Security error budget

Предпосылки

- Процесс исправления уязвимостей превращается в хаос



Security error budget

Предпосылки

- Процесс исправления уязвимостей превращается в хаос
- Нехватка времени в командах



Security error budget

Предпосылки

- Процесс исправления уязвимостей превращается в хаос
- Нехватка времени в командах
- Ресурсы тратятся на обсуждение, а не решение задач



Security error budget

1

2

3

4



Security error budget

1

Политика исправления

Crit — 4 hour fix

High — 2 days fix

Medium — 2 weeks fix

Low — half a year fix

2

3

4



Security error budget

1

Политика исправления

Crit — 4 hour fix
High — 2 days fix
Medium — 2 weeks fix
Low — half a year fix

2

Таблица стоимости

Crit — 1000$
High — 500$
Medium — 200$
Low — 50$

3

4



Security error budget

1

Политика исправления

Crit — 4 hour fix

High — 2 days fix

Medium — 2 weeks fix

Low — half a year fix

2

Таблица стоимости

Crit — 1000$

High — 500$

Medium — 200$

Low — 50$

3

Автоматизация

Установка due date

Подсчет error budget





Security error budget

1

Политика исправления

Crit — 4 hour fix

High — 2 days fix

Medium — 2 weeks fix

Low — half a year fix

2

Таблица стоимости

Crit — 1000$

High — 500$

Medium — 200$

Low — 50$

3

Автоматизация

Установка due date

Подсчет error budget

4

Контроль метрики

10 000$ / year



Security error budget

1 Политика исправления

- Crit — 4 hour fix
- High — 2 days fix
- Medium — 2 weeks fix
- Low — half a year fix

2 Таблица стоимости

- Crit — 1000$
- High — 500$
- Medium — 200$
- Low — 50$

3 Автоматизация

- Установка due date
- Подсчет error budget

4 Контроль метрики

10 000$ / year

Дополнительно:
автоматизация, автоматизация, визуализация и автоматизация

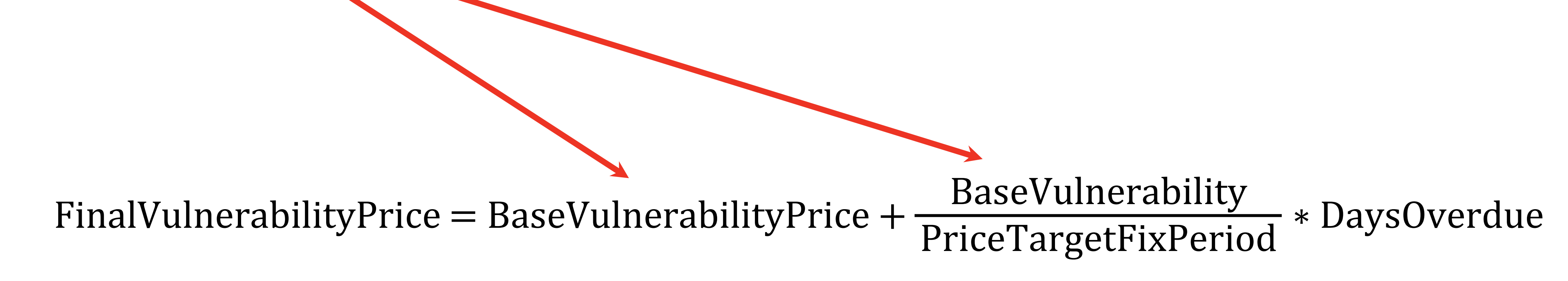


Security error budget

$$\text{BasedVulnerabilityPrice} = \text{CriticalityPrice} * \text{ThreatAssessmentCoefficient}$$



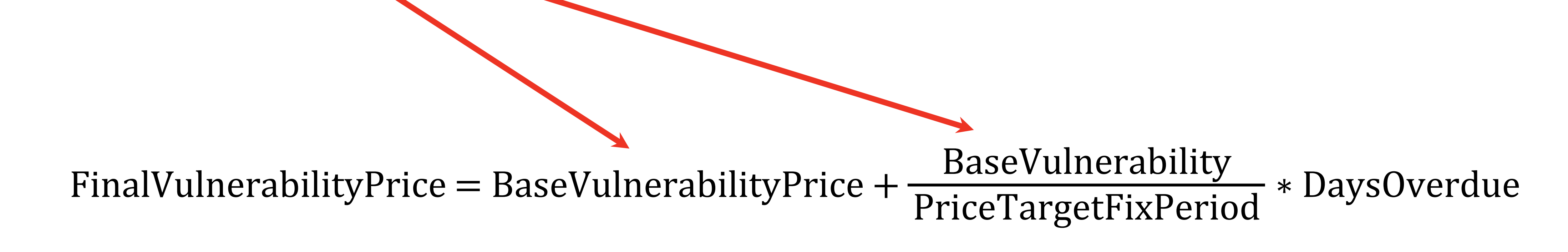
Security error budget





Security error budget

$$\text{BasedVulnerabilityPrice} = \text{CriticalityPrice} * \text{ThreatAssessmentCoefficient}$$



$$\text{Budget} = \sum_{i=1}^{N} \text{FinalVulnerabilityPrice}_i$$



Security error budget

Статус OKR	Команда	Приоретет...	Team Type	Взятый OKR / Комментарий
OKR принят	<Redacted>	important	Product	KR 1 Расход error-budget не выше 1000$



Security error budget



Automation for Jira July 28, 2022 at 4:43 PM

Due Date is set automatically based on Priority and Vulnerability Remediation Policy to 2022-09-26T13:43:07.8+0000

Edit · Delete ·



Security error budget

Error budget consumption by team



#	Assigned Team	Consupted budget	%
1	Team #4	1202420	58.1%
2	Team #2	423150	20.5%
3	Team #1	125400	6.1%
4	Team #10	119519	5.8%
5	Team #6	57418	2.8%
6 - 19	Show more...	140790	6.8%
Total		2068697	100%

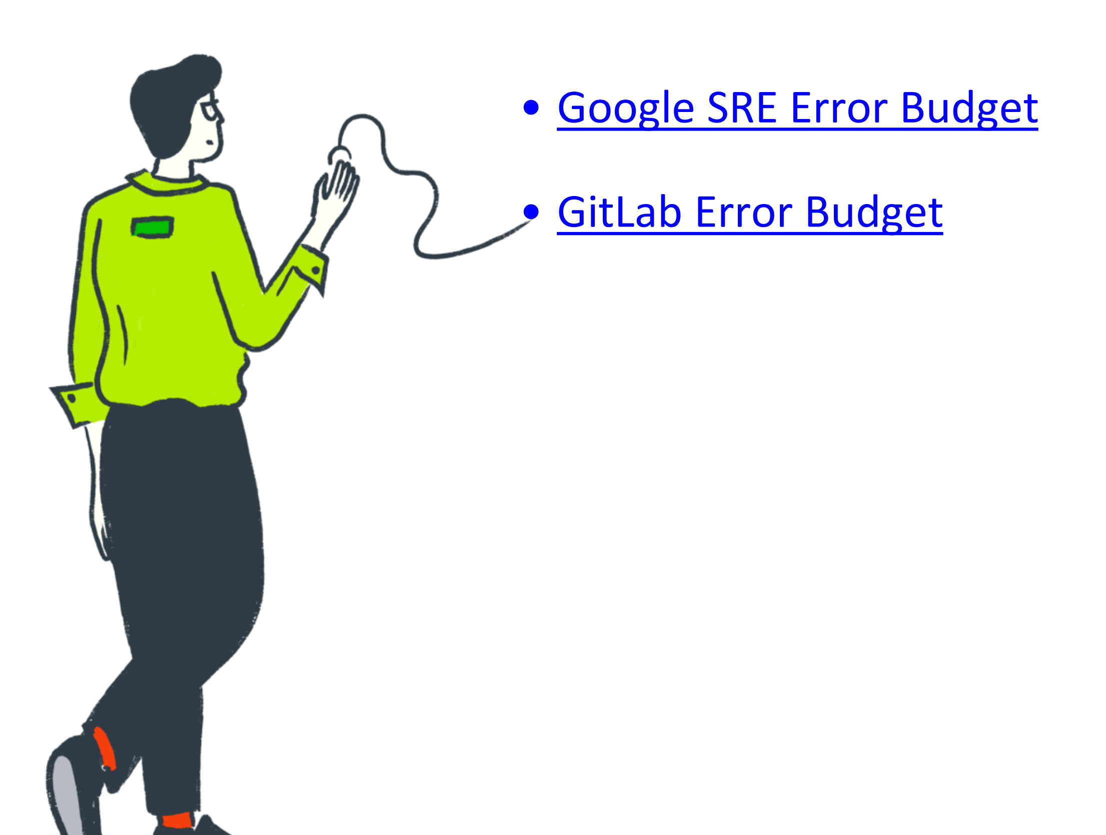
1202420

58.1%



Security error budget

Референс



- Google SRE Error Budget
- GitLab Error Budget



Security error budget

Флоу исправления уязвимостей

автоматизации

ИБ

Поиск и воспроизведение

фиксация в JIRA

консультации

верификация

написание регресса

Dev

исправление



Security-амбассадоры



Security-амбассадоры

Готовность повышать уровень знаний
в области безопасности в команде

Security Champions



Security-амбассадоры

Security Champions

- Не работает для всех команд



Security-амбассадоры

Security Champions

- Не работает для всех команд
- Чем больше требуется изменений, тем сложнее найти



Security-амбассадоры

Что даёт?

- Решение сложных проблем у сложных команд
- Сокращение расстояния до безопасности
- Уменьшение новых однотипных уязвимостей в команде

Связь с Конвеем

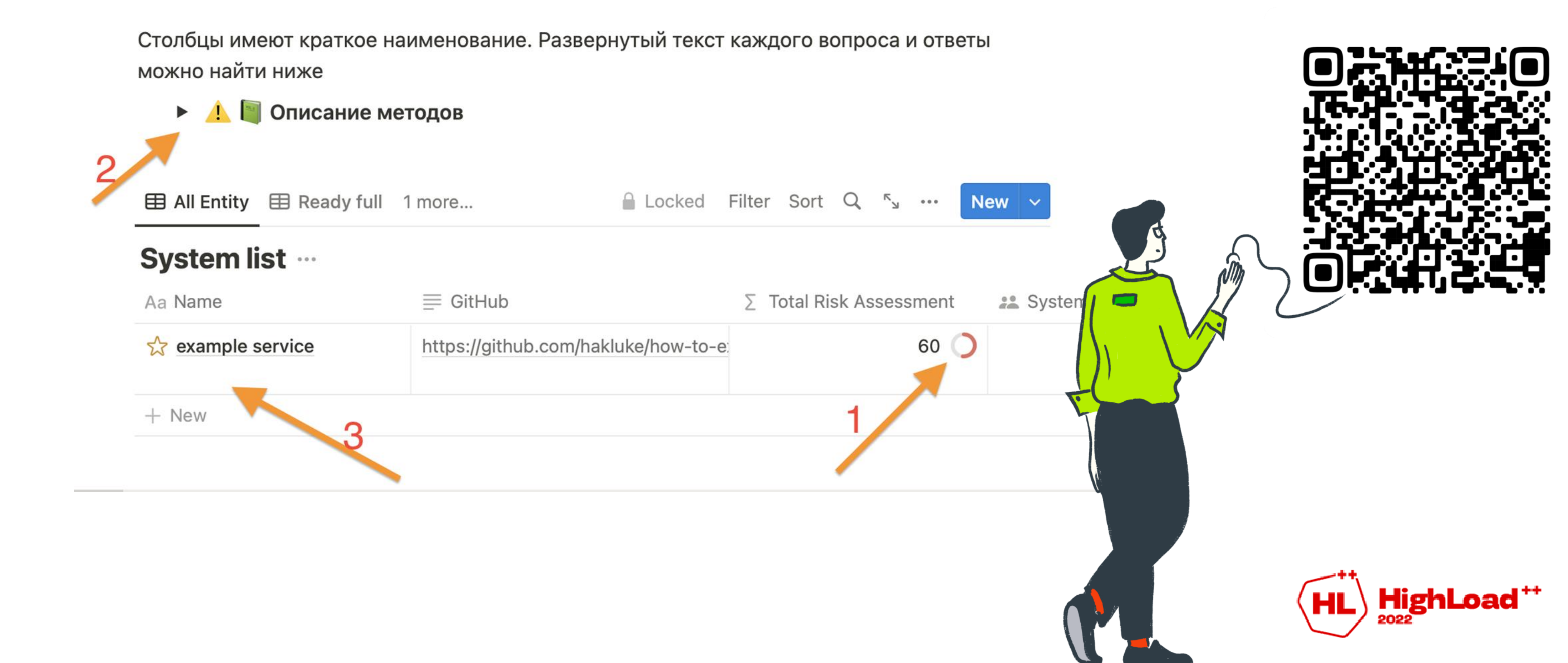
Способ упрощения коммуникации со сложными командами



Threat Assessment



Threat Assessment



Threat Assessment

Таблица Threat Assessm
инвентаризация

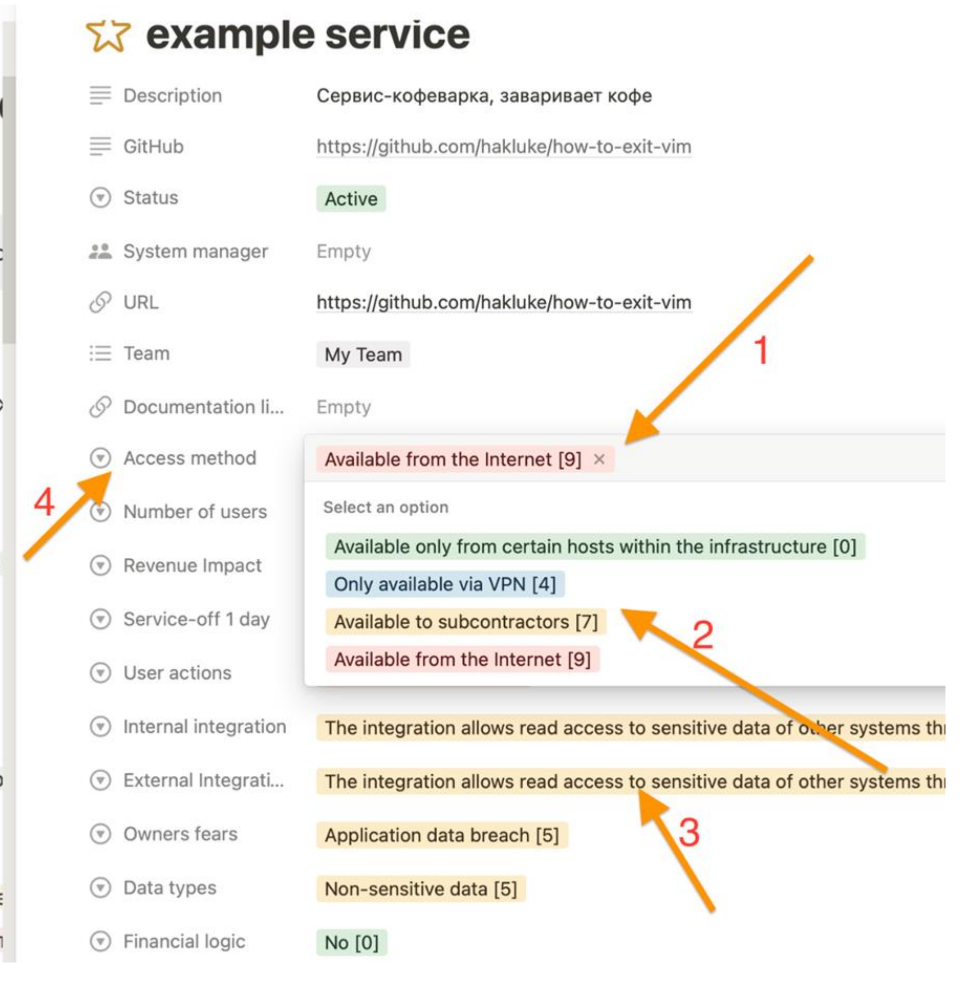
Опросник для инвентаризации создаваемых и текущих с

- Вводная информация по таблице
- Как внести информацию

Столбцы имеют краткое наименование. Развернутый текст ка
можно найти ниже

⚠️ 📗 Описание методов

1. Access method - Тип доступа пользователей
   a. Доступно только с определенных хостов внутри
   b. Доступно сотрудникам только за VPN
   c. Доступно субподрядчикам
   d. Доступно из Интернет
2. Number of users - Количество пользователей
   a. Сервисом пользуется мало людей, число пользо
   планируют развивать
   b. Сервисом пользуются сотрудники компании
   c. Сервисом пользуется до 70% клиентов/водителе
   d. Сервисом пользуется более 70% клиентов\водит





Threat Assessment

1

Направляем
анкеты лидам

2

Выделяем ТА, заполненные
без безопасника

3

Проводим интервью
со всеми, кто
не выслал в срок



Делаем переоценку
не реже, чем раз в год



Threat Assessment

Что даёт?

- Возможность считать метрики (WRT, DRW, Error Budget)
- Приоритеты на основе данных
- Выполнение требований ISO 27001

Связь с Конвеем

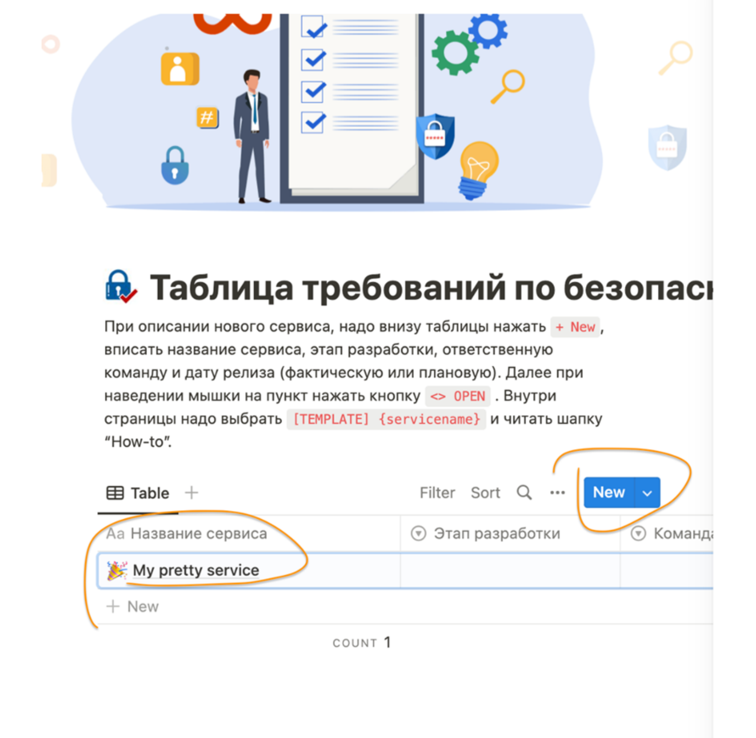
Позволяет команде осознать ответственность

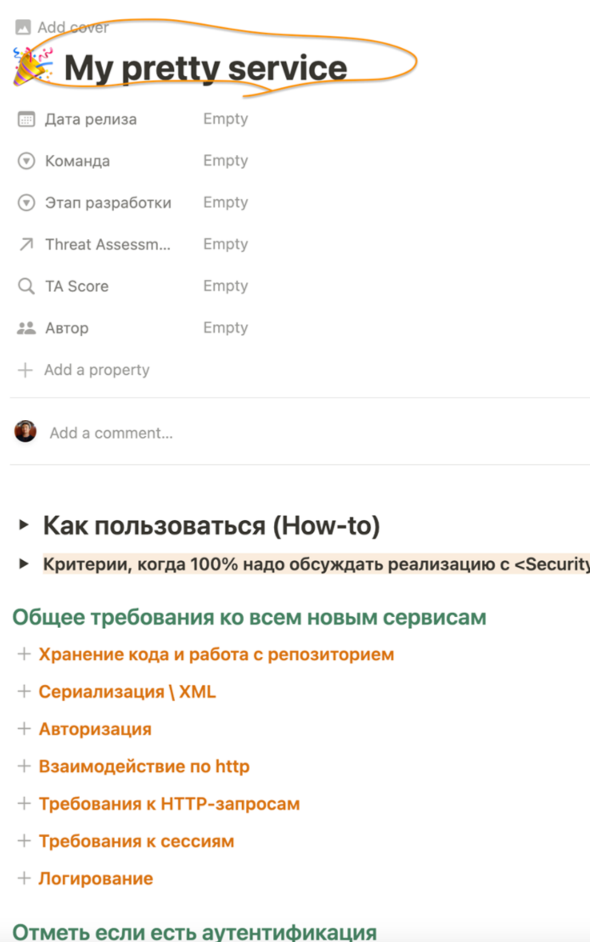


Security Architecture



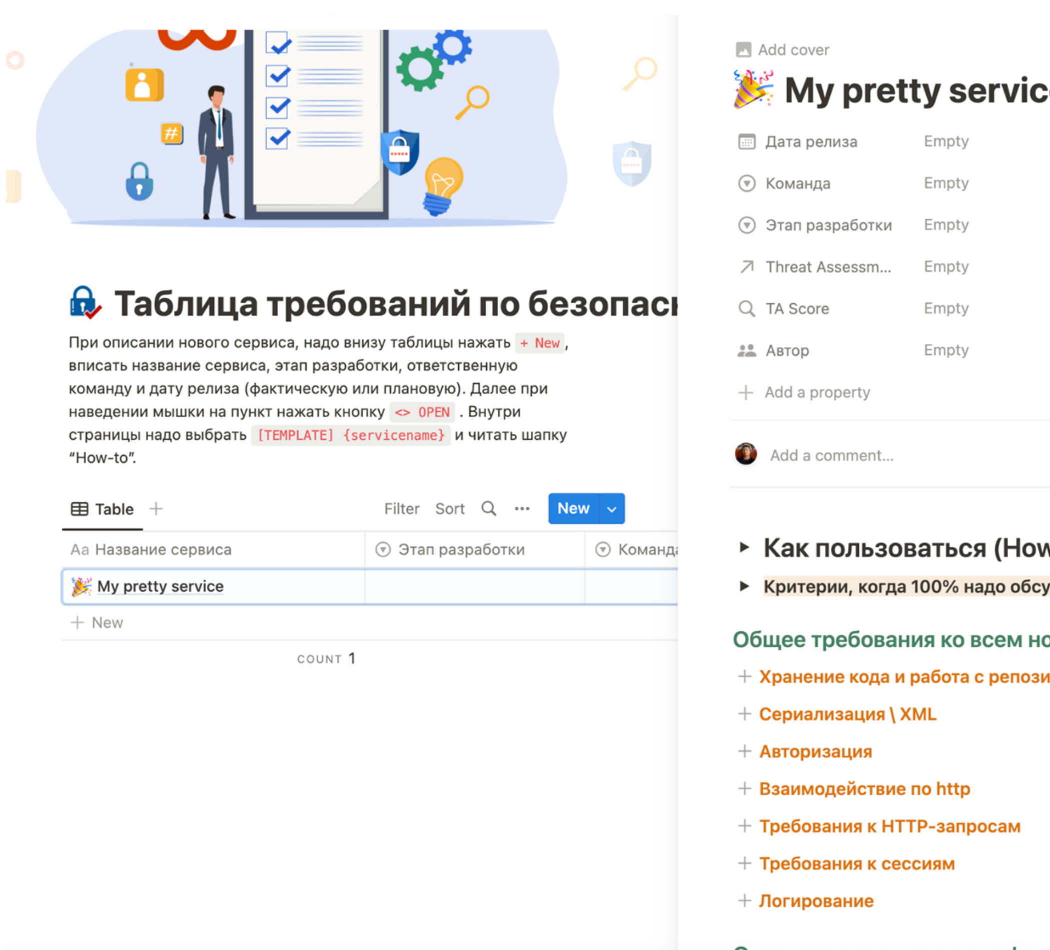
Security Architecture

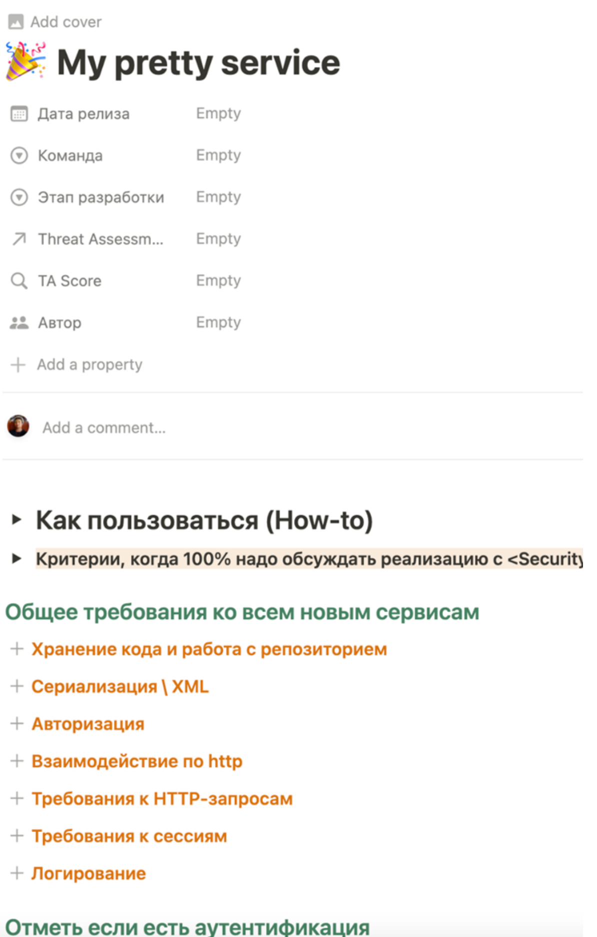






Security Architecture







Security Architecture

Таблица требований по безопасн

При описании нового сервиса, надо внизу таблицы нажать + New, вписать название сервиса, этап разработки, ответственную команду и дату релиза (фактическую или плановую). Далее при наведении мышки на пункт нажать кнопку <> OPEN . Внутри страницы надо выбрать [TEMPLATE] {servicename} и читать шапку "How-to".

Table + Filter Sort New

Aa Название сервиса	Этап разработки	Команда
My pretty service		

+ New

COUNT 1

Add cover

My pretty service

Дата релиза	Empty
Команда	Empty
Этап разработки	Empty
Threat Assessm...	Empty
TA Score	Empty
Автор	Empty

+ Add a property

Add a comment...

▸ Как пользоваться (How-to)

▸ Критерии, когда 100% надо обсуждать реализацию с <Security

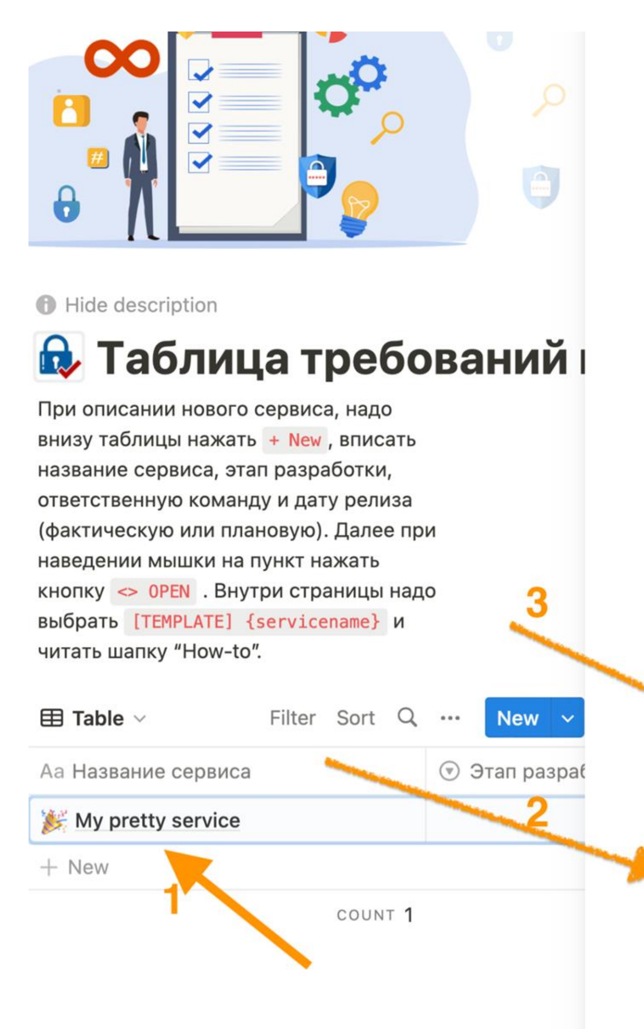
Общее требования ко всем новым сервисам

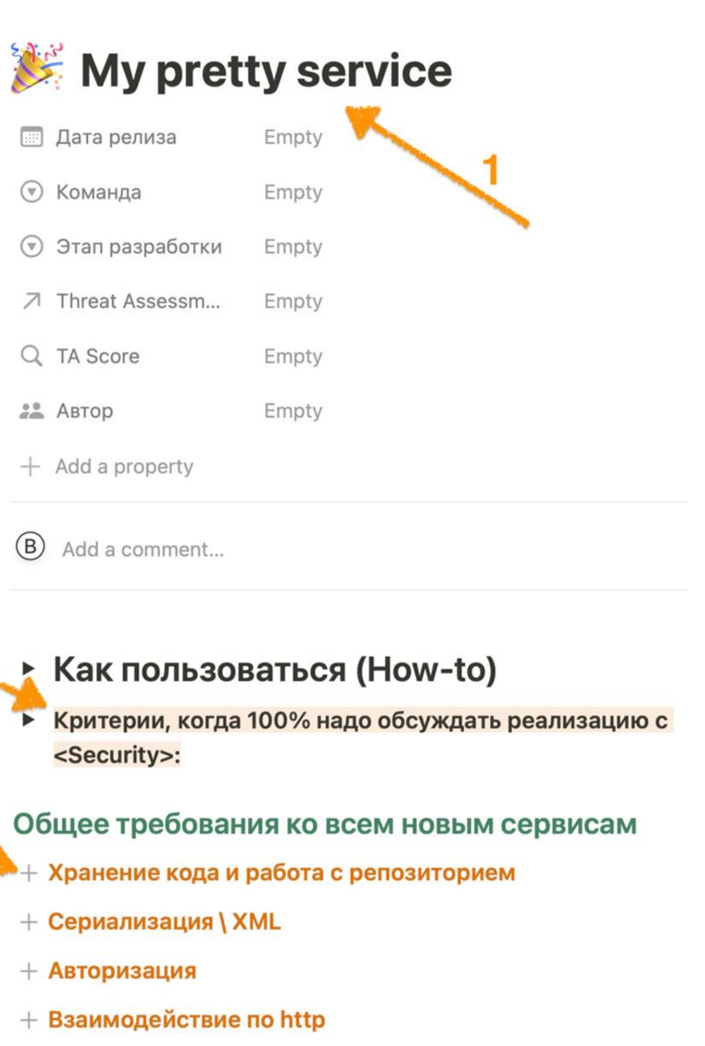
+ Хранение кода и работа с репозиторием
+ Сериализация \ XML
+ Авторизация
+ Взаимодействие по http
+ Требования к HTTP-запросам
+ Требования к сессиям
+ Логирование

Отметь если есть аутентификация



Security Architecture







Security Architecture

Отметь если есть аутентификация

+ **Базовые требования**

- [ ] При реализации механизмов аутентификации убедись что ты не строишь свой велосипед, когда есть уже готовый
- [ ] Любые внутренние "ручки" (эндпоинты) приложения должны проверять наличие сессии и права на выполнение данного действия у пользователя.

+ **Аутентификация с помощью паролей**

- [ ] Не используй аутентификацию по паролям не обсудим это с <Security>
- [ ] Для хеширования паролей используется алгоритм bcrypt
- [ ] Обдумай сценарий инвалидации сессий при смене пароля или предложи альетрнативы
- [ ] Ссылка для сброса пароля с токеном, должно жить не более 24ч.

+ **Общие требования по аутентифкации пользователей**

+ **Общие требования по аутентификации через OTP**

Секреты, токены

+ **Хранение**

+ **Валидация**

Отметь если используются файлы



Security Checklist



Security Checklist

Что даёт?

- Учёт регрессов по архитектуре
- Чек-лист для проверки реализации

Связь с Конвеем

Делаем архитектурный комитет комфортным для ИТ



Training days



Training Days





Training Days



Состав

- Тренировка BlueTeam
- Аудит сервиса
- Шаринг экспертизы



Training Days

Что даёт?

- Тренировка BlueTeam
- Шаринг экспертизы
- Выход за пределы повседневных задач

Как измерить?

- Найден хотя бы один инсайт
- Экспертиза пошарена на N человек
- Выявлены новые уязвимости
- Положительный фидбэк



Training Days

Что даёт?

- Тренировка BlueTeam
- Шаринг экспертизы
- Выход за пределы повседневных задач

Как измерить?

- Найден хотя бы один инсайт
- Экспертиза пошарена на N человек
- Выявлены новые уязвимости
- Положительный фидбэк

Связь с Конвеем

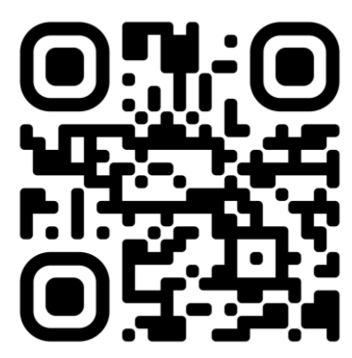
Решение проблемы межкомандного взаимодействия

Вопросы?

- Проекция закона Конвея на ИБ
- Cyber Strategy
- Security error budget
- Security амбассадоры
- Threat Assessment
- Security Architecture
- Training Days

```
{
  telegram: “t.me/edgesec”,
  github: “edgesecc”
}
```


profile_photo.png


indrive.tech.png



Обратная связь
и комментарии по
докладу по ссылке



